REMARKS

Applicants appreciate the thorough examination of the present application as reflected in the Official Action mailed April 22, 2004. Applicants have amended the specification to provide the serial number of the related case and to correct a typographic error. Applicants have amended Claims 29, 53 and 66 to clarify that the encryption key was used to encrypt the file. Applicants have also amended several claims to correct typographic errors in the claims. Applicants submit that the present application is in condition for allowance for the reasons discussed below.

The IDS

Applicants wish to bring to the attention of the Examiner an IDS that is being filed concurrently with the present Amendment. Applicants request that the Examiner consider the materials submitted and return an initialed copy of the PTO-1449 form with any subsequent communication.

The Claims Are Not Anticipated

Claims 1, 3-5, 9-20, 24-29, 31-44, 48-53 and 55-66 stand rejected under 35 U.S.C. § 102 as anticipated by United States Patent No. 5,499,298 to Narasimhalu et ` al. (hereinafter "Narasimhalu"). Official Action, p. 2. Of the Claims, Claims 1, 17, 29, 41, 53, 65 and 66 are independent claims. Applicants will first address each of the independent claims and then address the dependent claims. Applicants will address the independent claims in the order they were addressed in the Official Action.

Claim 17

Claim 17 stands rejected based on col. 5, lines 35-47, col.11, lines 1-5 and col. 6, lines 21-45 of Narasimhalu. Official Action, pp. 2-3. For the reasons discussed below, Applicants submit that Claim 17 is neither disclosed not suggested by the cited portions of Narasimhalu.

In particular, Claim 17 recites:

> 17. (Original) A method for controlling access to digital data of a file utilizing a file system including a personal key client, wherein the personal key client carries out the steps of:
> generating an encryption key;
> encrypting the digital data of the file with the encryption key;
> obtaining a password associated with the file;

generating a personal key from the password associated with the file;

encrypting the encryption key with the personal key;

incorporating in a file header the encryption key encrypted with the personal key;

requesting encryption of the file header with a control key;

receiving the file header encrypted with the control key;

associating the file header with the file; and

storing the file header and the encrypted digital data of the file at a file server.

Thus, in embodiments of the present invention as recited in Claim 17, three keys are used. A first key (the encryption key) is used to encrypt the digital data. A second key (the personal key), that is generated from the password, is used to encrypt the first key. The first key, encrypted with the second key, is incorporated in a file header and that file header is encrypted with a third key (the control key). By encrypting the encryption key with two different keys, file access may be controlled both by the owner of the personal key and the owner of the control key. Furthermore, as is clear from the recitations of Claim 17, the personal key client requests that the file header with the encrypted first key be encrypted with the third key (the control key) and receives the file header so encrypted. The file header encrypted with the third key is associated with the file and stored.

In contrast to the recitations of Claim 17, the cited portions of Narasimhalu describe a system where information is encrypted with a first key and that key is stored in the header unencrypted. See Narasimhalu, Fig. 4 and col. 6, lines 21-40. The header is then encrypted with a second key that is the access device's public key. See Narasimhalu, Fig. 2 and col. 6, lines 41-44. Thus, Narasimhalu appears to describe a system that uses only two keys, one that is used to encrypt the data and one that is used to encrypt the header. The key encrypted in the header does not appear to be an encrypted key as is recited in Claim 17. Thus, to access to the encrypted data the only decryption required is the decryption of the header to obtain the first key and of the data with the first key provided in the header.

If the encryption of the header in Narasimhalu is interpreted as providing the encryption by the control key as recited in Claim 17, then the cited portions of Narasimhalu do not disclose encryption by the personal key of Claim 17. Similarly, if the encryption of the header in Narasimhalu is interpreted as providing the encryption

of the key used to encrypt the data by the personal key as recited in Claim 17, then the cited portions of Narasimhalu do not disclose encryption by the control key of Claim 17. Such is the case because, as discussed above, Narasimhalu only describes the use of two encryption keys whereas Claim 17 recited the use of three encryption keys. Accordingly, Applicants submit that Claim 17 is not anticipated by Narasimhalu.

Claim 29

Claim 29 stands rejected based on col. 5, lines 4-15 and 35-47, col. 6, lines 1-15 of Narasimhalu. Official Action, p. 6. For the reasons discussed below, Applicants submit that Claim 29 is neither disclosed not suggested by the cited portions of Narasimhalu.

Claim 29 recites:

> 29. (Currently Amended) A method for controlling access to digital data of a file in a file system having a personal key server, the personal key server carrying out the steps of:
> receiving a request from a requestor to create a file header associated with the file, the request containing an encryption key utilized to encrypt the digital data, the encryption key being encrypted with a personal key;
> encrypting the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and
> returning the file header to the requestor.

Thus, Claim 29 also provides for three encryption keys. As discussed above, Narasimhalu describes the use of two keys, not three. Accordingly, Applicants submit that Claim 29 is patentable over Narasimhalu at least for reasons analogous to those discussed above with reference to Claim 17.

Claim 1

Claim 1 stands rejected based on Nirasimhalu for the same reasons as Claims 17 and 29. Official Action, p. 9. Applicants, submit that Claim 1 is patentable over Nirasimhalu for reasons analogous to those discussed above with reference to Claim 17. Applicants further submit that the system recitations of Claim 1 are also not disclosed or suggested by the cited portions of Nirasimhalu.

For example, Claim 1 recites:

> 1. (Currently Amended) A system for controlling access to digital data of a file, the system comprising:

a file server configured to store an encrypted file and a file header corresponding to the digital data of the file and containing an encryption key encrypted with both a personal key of an owner of the file and a control key;

a personal key server configured to receive a header associated with a file, the file header containing an encryption key encrypted with a personal key and encrypt the encrypted encryption key with a control key to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

a personal key client configured to generate the encryption key, encrypt the digital data of the file with the encryption key, generate the personal key from a password associated with the file, encrypt the encryption key with the personal key, incorporate the encrypted encryption key in a file header associated with the file and provide the file header with the encryption key encrypted with the personal key to the personal key server, receive the file header from the personal key server and provide the file header received from the personal key server to the file server.

Thus, the system of Claim 1 includes three components, a file server, a personal key server and a personal key client. The personal key server receives headers and encrypts the header with a control key. The personal key client encrypts the data with an encryption key, encrypts the encryption key with a personal key and provides the encrypted encryption key in a file header to be encrypted by the personal key server.

In contrast, in the cited portions of Narasimhalu, it appears that all of the encryption operations are carried out by the information provider. Thus, for example, all of the operations of Figure 4 of Narasimhalu are described as being carried out by the Information Provider 10 of Figure 1. See Narasimhalu, col. 6, lines 24-26. Thus, the cited portions of Narasimhalu fail to disclose the different components recited in Claim 1. As such, Applicants submit that Claim 1 is patentable over the cited portions of Narasimhalu for at least these additional reasons.

Claims 41, 53, 65 and 66

Claims 41, 53, 65 and 66 are system and computer program product claims corresponding to Claims 17 and 29. Applicants submit that these claims are patentable over Narasimhalu for reasons analogous to those discussed above with reference to Claims 17 and 29.

The Dependent Claims

Applicants submit that the dependent claims are patentable at least as depending from a patentable base claim. Applicants also submit that certain of the dependent claims are not disclosed or suggested by Narasimhalu. For example, Claim 19 recites:

> extracting the encryption key encrypted with the personal key and the control key from the file header;
> requesting recovery of the encrypted encryption key from the file header;
> receiving the recovered encrypted encryption key;
> obtaining a password to decrypt the file;
> generating the personal key from the obtained password;
> decrypting the recovered encrypted encryption key with the personal key to recover the encryption key; and
> decrypting the encrypted digital data with the recovered encryption key.

However, as discussed above, the cited portions of Narasimhalu do not describe "an encryption key encrypted with a personal key and a control key as recited in Claim 19.

Furthermore, in rejecting Claim 19, the Official Action cites to portions of Narasimhalu that describe different embodiments of Narasimhalu out of context. See Official Action, p. 3. For example, the citation to col. 7 of Narasimhalu relates to a first embodiment whereas the citation to col. 11, lines 1-5 describes operations for providing an "Opener" that is provided separate from the file according to a second embodiment. With regard to the "Opener", the encryption of the file and header appears to be described at col. 10, lines 48-65 and in Fig. 8 of Narasimhalu. The "Opener" appears to be a way to provide the key that was used to encrypt the header of the file and does not appear to further encrypt the header or the key contained in the header. See e.g. Narasimhalu, col. 10, line 66 to col. 11, line 11.

The Official Action also equates the "CID" of Narasimhalu with the password to Claim 19. Official Action, p. 3. However, the CID of Narasimhalu is not used to generate a personal key as recited in Claim 19. The CID is a unique identifier of a contract of information dissemination and is not described as being used to generate a key. See Narasimhalu, col. 9, lines 32-34. Accordingly, Applicants submit that the generation of the personal key as recited in Claim 19 is also not disclosed or suggested by the cited portions of Narasimhalu.

In light of the above discussion, Applicants submit that Claim 19 is separately patentable for at least these additional reasons. Analogous arguments may also be made with respect to Claim 20. Furthermore, contrary to the assertions of the Official Action at page 4 with regard to Claim 20, re-encrypting the data with a new key is not generating a personal key from a new password as recited in Claim 20. Accordingly, Claim 20 is also separately patentable for at least these additional reasons.

Claim 26 recites encrypting the encryption key with a public key of each authorized user other than the owner of the file and incorporating these encrypted keys in the header. The Official Action cites to col. 6, lines 1-12 as teaching the recitations of Claim 26. Official Action, p. 5. However, this portion of Narasimhalu is merely a general description of public key cryptography. There is no indication that a key used to encrypt a file is encrypted with a public key of each authorized user and these encrypted keys are placed in the header associated with the file. As such, Applicants submit that Claim 26 is separately patentable for at least these additional reasons. Analogous arguments may be made with reference to Claims 28 and 37.

Claim 27 recites encrypting the recovered encryption key with a new public key associated with a user. The Official Action cites to col. 11, lines 31-60 of Narasimhalu as disclosing the recitations of Claim 27. Official Action, p. 5. However, the cited portion of Narasimhalu describes using a new key to encrypt the COIN, i.e. the data, not the header. The key utilized to encrypt the header does not appear to be changed. See Narasimhalu, col. 11, lines 52-55. As such, Applicants submit that the cited portion of Narasimhalu does not disclose or suggest the recitations of Claim 27 and, therefore, Claim 27 is separately patentable for at least these additional reasons.

Applicants further submit that certain dependent claims depending from Claim 1 are also separately patentable at least for reasons analogous to those discussed above. In the interest of brevity, those arguments will not be repeated here.

The Claims Are Not Obvious

Claims 6-8, 21-23 and 45-47 stand rejected under 35 U.S.C. § 103 as obvious in light of Narasimhalu and United States Patent No. 6,105,131 to Carroll (hereinafter "Carroll"). Claims 2, 30 and 55 stand rejected under 35 U.S.C. § 103 as obvious in

light of Narasimhalu and United States Patent No. 6,678,731 to Howard et al. (hereinafter "Howard"). Applicants submit that these claims are patentable at least as depending from a patentable base claim.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned for under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to Deposit Account No. 09-0461.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

USPTO Customer No. 20792

Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401